AMENDMENTS TO THE CLAIMS

Below is the entire set of pending claims pursuant to 37 C.F.R §1.121(c)(3)(i), with any mark-ups showing the changes made by the present Amendment.

1. (Presently amended) A security system for controlling access to encrypted information, comprising:

a hardware device for storing at least one decryption key for use in decrypting an encrypted item of information, the decryption key being associated with a security code which is used by the hardware device to determine whether it is authorised to send encrypted copies of the decryption key to others, wherein if the hardware device is authorised to send an encrypted copy of the decryption key, it encrypts the decryption key and propagates the encrypted copy of the decryption key, wherein each time the hardware device propagates a decryption key, it includes as part of the decryption key an identifier indicating the identity of a sender's key, and wherein a user can append a control word against their identity in the decryption key to instruct the hardware device to initiate a message to them or an agent informing them of the propagation of the key and giving information concerning that propagation.

2. (Original) The security system of claim 1, wherein if the hardware device is authorised to send an encrypted copy of the decryption key to a first entity, it encrypts the decryption key using an encryption key associated with the first entity.

3. (Original) The security system of claim 2, wherein the decryption key is encrypted with a public key of the first entity.

4. (Original) The security system of claim 1, wherein each time the hardware device sends a decryption key to another entity, it modifies the security code associated with the decryption key and sends the modified security code as part of the encrypted decryption key.

5. (Original) The security system of claim 4, wherein the security code is a numeric value indicating the number of times the encryption key can be propagated, and the security code is decremented each time the decryption key is propagated to a further entity.

6. (Original) The security system of claim 1 wherein the decryption key is stored within the hardware device.

7. (Original) The security system of claim 1, wherein the hardware device is removable from a data processor.

8. (Original) The security system of claim 1, wherein the hardware device is in the form of a user unit, which, in use, a user introduces to a data processor when the user wishes to use the data processor to access encrypted information and removes the user unit from the data processor when the user has finished.

9. (Cancelled)

10. (Presently amended) The security system of claim 1~~9~~, wherein the decryption key includes an audit trail of individuals who have allowed propagation of the key.

11. (Cancelled)

12. (Original) The security system of claim 1, wherein the decryption key is passed between a plurality of hardware device.

13. (Original) The security system of claim 1, wherein a user's private key is stored within their own hardware device, such that the encrypted decryption key can only be decrypted when the hardware device is in operation.

14. (Original) The security system of claim 1, wherein the hardware device includes a data processor such that all encryption and decryption of the decryption keys is performed within the hardware device.

15. (Presently amended) A method of controlling ~~the~~ propagation of a decryption key that allows ~~keys for allowing~~ access to encrypted data, the method comprising the steps of:

associating the ~~a~~ propagation control word with a decryption key for an item of data, and in response to an instruction to send the key to a specified recipient, checking the status of the control word to determine if propagation is allowed, and if so, modifying the control word and encrypting the control word and decryption key with a recipient's public key and sending the encrypted key, including as part of the decryption key an identifier indicating the identity of a sender's key, and appending a control word against a user's identity in the decryption key to instruct a hardware device to initiate a message to them or an agent informing them of the propagation of the key and giving information concerning that propagation.

16. (Presently amended) The method of claim 15, wherein the control word is a numeric value which is decremented at each propagation, and wherein ~~in which~~ propagation is inhibited once the numeric value reaches a predetermined value.

17. (Presently amended) A method of claim 15, wherein an ~~the~~ originator of the decryption ~~a~~ key sets a maximum ~~the~~ number of times the key can be sent, and each time a key is sent, a variable holding a generation number of the key is modified such that when the generation number reaches the maximum number of times the key can be sent, further sending of the key is inhibited.

18. (New) A security system for controlling access to encrypted information by a plurality of users, comprising a hardware device for storing at least one data unit comprising a decryption key and an associated security code, in which the decryption key is used in decrypting an

encrypted item of information and the security code controls the number of times that the decryption key can be propagated, and the hardware device examines the security code which code includes a group code as an indication of an acceptable range of recipients to determine whether it is authorized to send encrypted copies of the decryption key to those recipients, wherein if the hardware device is authorized to send an encrypted copy of the decryption key, it encrypts the decryption key and propagates the encrypted copy of the decryption key.

19. (New) A security system of claim 18, wherein if the hardware device is authorised to send an encrypted copy of the decryption key to a first entity, it encrypts the decryption key using an encryption key associated with the first entity.

20. (New) A security system of claim 19, wherein the decryption key is encrypted with a public key of the first entity.

21. (New) A security system of claim 18, wherein each time the hardware device sends a decryption key to another entity, it modifies the security code associated with the decryption key and sends the modified security code as part of the encrypted decryption key.

22. (New) A security system of claim 21, wherein the security code is a numeric value indicating the number of times the encryption key can be propagated, and the security code is decremented each time the decryption key is propagated to a further entity.

23. (New) A security system of claim 18, wherein the decryption key is stored within the hardware device.

24. (New) A security system of claim 18, wherein the hardware device is removable from a data processor.

25. (New) A security system of claim 18, wherein the hardware device is in the form of a user unit, that a user introduces to a data processor when the user wishes to use the data processor to access encrypted information and removes the user unit from the data processor when the user has finished.

26. (New) A security system of claim 18, wherein each time the hardware device propagates a decryption key, it includes as part of the key an identifier indicating the identity of the sender's key.

27. (New) A security system of claim 18, wherein the decryption key includes an audit trail of individuals who have allowed propagation of the key.

28. (New) A security system of claim 18, wherein a user can append a control word against their identity in the decryption key to instruct the hardware device to initiate a message to them or an agent informing them of the propagation of the key and giving information concerning that propagation.

29. (New) A security system of claim 18, wherein the decryption key is passed between a plurality of hardware devices.

30. (New) A security system of claim 18, wherein a user's private key is stored within their own hardware device, such that the encrypted decryption key can only be decrypted when the hardware device is in operation.

31. (New) A security system of claim 18, wherein the hardware device includes a data processor such that all encryption and decryption of the decryption keys is performed within the hardware device.

32. (New) A method of controlling the propagation of decryption keys to a plurality of users for allowing access to encrypted data, comprising the steps of storing at least one data unit on a hardware device, the at least one data unit comprising a decryption key, including a propagation control word with the decryption key in the data unit, and in response to an instruction to send the data unit to a specified recipient, checking the status of the control word to determine if propagation is allowed, including checking that the specified recipient is within an acceptable range of recipients indicated as a group code in the control word, and if so, modifying the control word and encrypting the data unit comprising the control word and decryption key with a recipient's public key and sending the data unit.

33. (New) A method of claim 32, wherein the control word is a numeric value which is decremented at each propagation, and wherein propagation is inhibited once the numeric value reaches a predetermined value.

34. (New) The method of claim 32, wherein an originator of the decryption key sets a maximum number of times the key can be sent, and each time the key is sent, a variable holding a generation number of the key is modified such that when the generation numbers reaches the maximum number of times the key can be sent, further sending of the key is inhibited.